Assurance for Service Organisations

Channuntapipat, Charika

DOI:
10.1108/MAJ-06-2017-1588

Document Version
Peer reviewed version

Citation for published version (Harvard):
Channuntapipat, C 2017, 'Assurance for Service Organisations: Contextualising Accountability and Trust', *Managerial Auditing Journal*, vol. 33, no. 4, pp. 340-359. https://doi.org/10.1108/MAJ-06-2017-1588

Managerial Auditing Journal

Assurance for Service Organisations: Contextualising Accountability and Trust

Journal:	*Managerial Auditing Journal*
Manuscript ID	MAJ-06-2017-1588.R1
Manuscript Type:	Research Paper
Keywords:	service organisation, accountability, trust, voluntary assurance

Assurance for Service Organisations: Contextualising Accountability and Trust

Abstract

Purpose – A number of organisations outsource their information systems and information technology infrastructure to a type of organisation called a "service organisation". In the current business environment, where cyber risks are increasing, it is important to have a mechanism to ensure the credibility of these service organisations. This paper, therefore, aims to understand the contextualisation of accountability and trust of related organisations through the use of assurance engagements.

Design/methodology/approach – This paper is conceptual in nature; however, textual data sources are used to support the theorisation of accountability and trust in the context of companies using service organisations. It employs publicly available assurance reports and related assurance standards for observing the accountability mechanism in practice, in order to understand the purpose of the assurance.

Findings – Assurance statements for service organisations mainly provide reputation-based, not contract-based, accountability. Limited access to the assurance reports and limited responsibility of service auditors potentially decrease the degree of this reputation-based accountability. The findings reveal a potential accountability paradox regarding the role of assurance practice, as to whether it serves as a managerial tool to build trust or as an accountability mechanism for stakeholders.

Originality/value – This paper extends our understanding of accountability and trust in the context of this unconventional form of organisational relationship. It urges more transparency in terms of the accessibility of assurance reports to provide information to wider stakeholders. The findings add to the latent literature on organisational trust and voluntary~~non-financial~~ assurance practice.

Keywords – service organisation, ~~non-financial~~voluntary assurance, accountability, trust

Paper type – research paper

1. Introduction

In the current decade, the advancement of information technology has influenced the change in how companies store and process all kinds of data, including their business transaction information and clients' personal data. A number of companies have outsourced their information technology infrastructure and data storage to organisation, so called 'service organisations'. The term 'service organisation' refers to an organisation that provides outsourcing services to entities aiming to contain or reduce costs.

A number of organisations outsource some of their operational functions relating to information technology, accounting, customer care, human resources, benefits management, payments and so on. This outsourcing can benefit organisations, allowing them to have better operational systems and to achieve technological improvement and cost savings. However, the benefits do not come without risks. Those risks include lack of compliance with contracts, loss of technical knowledge, and potential non-financial costs (Gonzalez et al., 2010), especially risks relating to information technology systems.

This outsourcing activity can affect the operation and internal control of entities if adequate~~internal~~ controls are not in place in the service organisations. This means service organisations are the entity's supplier, while the entity is a supplier of the end clients/users. This, in turn, means service organisations have become instrumental in the quest to fulfil promises to entities' stakeholders along the supply chain.

For example, a company using cloud computing services needs to make sure that the service organisation providing the cloud service has appropriate controls to protect their business, client and other types of data. Thus, certification and compliance with regard to information security standards, compliance with regulations, and auditing norms have been introduced and may be required by the user organisation (Panth et al., 2014).

It is worth noting the terms relevant to several roles involved in this outsourcing environment.

> ***User organisation:*** an entity that has outsourced part of its business to a service organisation.
>
> ***User auditor:*** an auditor of the user organisation.
>
> ***Service organisation:*** a provider of a service to a user organisation that is likely to be relevant to the user organisation's internal control.
>
> ***Service auditor:*** an auditor of the service organisation.

The relationships among these parties challenge the conventional agent-principal relationship and the accountability model that is associated with it. The responsibility of service organisations is not clear. Also, unlike financial audit reports that are commissioned by the principal to mitigate the potential that the agent is going to serve their own interests, the assurance for a service organisation is mainly commissioned by the management of that service organisation. This introduces issues of the role of this kind of assurance and issues relating to the interplay

between accountability, trust and reputation of user organisations, service organisation, and service auditors.

This paper aims to seek the answer to the question: "What is the purpose of assurance for service organisations?" The key question is whether current practice in assurance in service organisations is serving to enhance accountability, or is serving other purposes? If it does serve accountability, then who are the accountable parties? By adopting the accountability framework developed by Swift (2001), this paper highlights the roles of assurance statements for service organisations in relation to accountability and trust. It focuses on the purposes of the assurance engagement and the communication of the assurance to related stakeholders. The discussion from this paper is fundamental to information technology governance and digital trust. This could potentially provide a stepping stone to understanding the relevant assurance practices and stakeholders' trust relating to cyber security risks that are prevalent in this business environment addressed in this paper.

This paper is divided into a further five sections. The next section discusses the nature of assurance practice for service organisations. The section includes the description of relations between related parties, assurance in service organisations as a voluntary ~~non-financial~~ assurance practice, and related assurance standards. The conceptual framework is then presented. Next, example cases to illustrate the assurance practice and the use of assurance reports are discussed. This is followed by discussion of the public disclosure of assurance statements, accountability, and stakeholders' trust. The paper finishes with concluding sections.

2. Service organisations and the assurance practice

The fast pace of technological evolution, big data technology and standardised business processes influence companies in outsourcing some parts of their information systems. Although the outsourcing trend has been around for years now, it is still being more widely adopted. Outsourcing refers to any task, operation, or process of an organisation that is done by a third party, or another service organisation.

The use of service organisations requires user organisations to better manage their risks relating to the outsourced services. The user organisation, therefore, requires a certain degree of assurance that the service organisation has well-established internal controls that can be aligned with their own internal controls and other requirements. Therefore, user organisations and the users' auditors need to send requirements to service organisations asking for such assurance to ensure the efficiency and effectiveness of their internal controls. This is where assurance practice within service organisations plays an important role as an accountability and trust mechanism. Assurance or review of third party service providers, or service organisations, can be conducted to satisfy the requirements of user organisations in terms of outsourcing contracts and data security.

Although tasks are outsourced to service organisations, the accountability of user organisations cannot really be outsourced. In other words, user organisations are ultimately responsible for

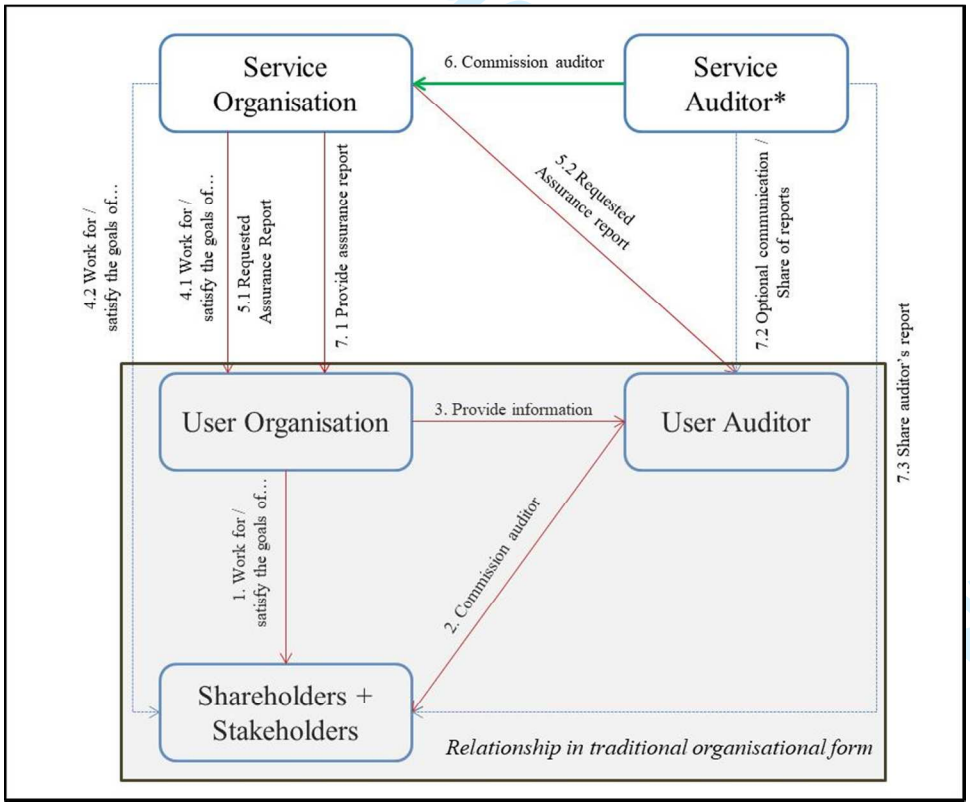
their control environment, which is affected by the use of service organisations. This influences the increasing demand for control assurance for activities performed by third parties.

Problems might arise when the process of holding a user organisation accountable to their stakeholders involves two sets of control relationships (i.e. 1. user organisation and stakeholders, and 2. user organisation and service organisation). The problems are visible in this new form of organisational relationship (i.e. outsourcing) (Child and Rodrigues, 2003).

2.1 Relationship between user entity, service organisation, and their auditors

This section aims to illustrate the relationship between different parties involved in outsourcing activities and the assurance practice in service organisations. There may be more than one level of service organisation, meaning that the service organisation outsources parts of their tasks and processes to another service organisation (i.e. subservice organisation). However, in this paper, only one level of service organisation is illustrated because the relation between subservice organisations with other related parties will be similar to those of the service organisation with those parties. Figure 1 shows the relationship between those parties.

Figure 1: Relationships between service organisations and other entities.



(Adapted from Knolmayer and Asprion (2011))

The highlighted area in the diagram shows the relationships in a traditional organisational form without outsourcing activities. An arrow represents the service flow, starting from the party that provides services (including information, and reports) to another party, which is at head of the arrow.

From the diagram shown in Figure 1, it can be seen that there is a service organisation with its auditor added to the traditional diagram showing the relationship between agent, principal, and auditor. The relationship in the traditional organisational form starts where an (user) organisation operates to serve the goals of its shareholders and stakeholders. Due to the assumptions of agency theory that management of an organisation will pursue self-interest and that there is information asymmetry between the organisation and shareholders, an accountability mechanism needs to be implemented. An (user) auditor, having their duty to shareholders, conducts the audit of the user organisation's financial statements, and the auditing practice serves as a mechanism to enforce the accountability of the organisation.

When the picture includes a service organisation, the relationship between related parties becomes more complex. The outsourcing of activities means that a user organisation is the direct client of a service organisation, and that this service organisation needs to serve the goals of the user organisation in the commissioned areas. The question is whether the service organisation is also accountable to the shareholders and stakeholders of the user organisation. Due to concern about internal controls in service organisations, which may affect the operation of their services, a user organisation requires from the service organisation assurance regarding its internal controls (the request can also come from a user auditor). The service organisation then needs to commission independent assurance for its internal controls. The assurance report is then provided to the user organisation and, in some cases, to the public so that anyone can see the report.

Problems of agency and accountability can arise because of the greater complexity of this new form of organisational relationship, compared to the traditional relationship of a single agent and a single principal. This form of relationship raises the following issues regarding accountability in terms of both legal and social contractual relationships:

- To whom are service organisations accountable?
- To whom is the service auditor accountable?
- Does the user organisation trust the service organisation, or the service auditor, so that it decides to use the services of the service organisation?
- To which entity should shareholders / stakeholders give more trust?

This introduces the paradox of accountability, because accountability based on agent-principal terms refers to the duty to provide an account of an agent's actions for the principal, to whom the agent is responsible (Roberts and Scapens, 1985). Thus, the agent-principal framework assumes a narrow conception of accountability, which is pertinent to contractual agreements between the two parties. However, accountability can be variously defined as more inclusive of other stakeholders, or as pertinent to a "social contract" (Gray et al., 1988).

The next section provides a brief introduction to non-financial assurance and assurance for service organisations as a part of non-financial assurance practice. This will be linked to the trust produced by assurance providers and assurance reports for other parties.

2.2 ~~Non-financial~~ Voluntary assurance and trust

The extent to which entities engage in voluntary ~~non-financial~~ assurance practices is apparent through the increasing risks that organisations are facing in the new business environment~~importance of non-financial information~~; and increasing number of such assurance services and assurance statements accompanying various kinds of ~~non-financial~~corporate reports. It might be assumed that the increasing amount of ~~non-financial~~corporate reports and assurance statements indicate that more organisations are being held accountable for the impacts of their operations on related stakeholders (Swift, 2001).

Assurance for service organisations is considered as one of the ~~non-financial~~voluntary assurance practices~~, but services related to~~ because ~~this practice are~~it is largely unregulated. One of the main issues for ~~non-financial~~these assurance services is expertise in specific subject matters relevant to a particular practice. However, the main aim of the assurance remains the same as for financial assurance, which is to increase the relevance and reliability of the assured non-financial information (Elliott, 1977).

Barrett and Gendron (2006) and Gendron and Barrett (2004), for example, look at how e-commerce assurance, called WebTrust, is developed to enhance digital trust in the clients' websites. These studies show the attempts of assurance providers to develop this voluntary non-financial assurance service and to persuade ~~reporting~~ organisations operating in such environment to engage with their services. Understanding that the roles played by assurance providers reflect how they serve, and are responsible to, different stakeholders (Power and Terziovski, 2007), allows the purpose of the assurance to be inferred. Power (1996) discusses three types of non-financial audits, quality audit, research audit, and brand audit, in order to understand the logic of auditability and the creation of an audit environment. Something is perceived to be auditable if it creates a network of trust and an auditability environment. Audit methodologies are believed to work because they are institutionally accepted through the process of negotiation of audit expertise. Subjects that are perceived as unauditable could become auditable at a later period because the network of trust and the auditability environment has been created around them (Power, 1996).

Knolmayer and Asprion (2011) discuss the assurance practices for IT subcontracting and cloud computing. They call more attention to controls over privacy of non-financial data, and the need for increasing regulation on the IT outsourcing, especially in the business environment where cyber security issues are prevalent. As the relevant assurance practices for IT outsourcing have been changed from audit function (SAS70) to attestation function (ISAE3402 / SSAE 16) (Bierce and Kenerson, 2010), this nature of assurance practice might decrease the level of comfort and trust from the users of this kind of assurance reports (Knolmayer and Asprion, 2011, pp.32). Still, the main function of assurance practice, whether it is audit or attestation, is to create

trust on the audited subjects. In the digital age where cyber security is one of the major concerns for every organisation and their stakeholders, digital trust in such environment needs to be built and maintained. Thus, assurance might be needed for such purposes.

As there are a number of assurance practices and assurance standards that can be related to IT outsourcing and cyber security, this paper focuses on a particular assurance practice called assurance for service organisations because this assurance practice relates to the broader business environment where companies outsource their particular functions, and also to IT governance of the outsourcing and service organisations.

~~Ferguson and Pündrich (2015) have conducted a study to consider whether industry specialisation with respect to assurance for non-financial information matters to investors. There is weak evidence to suggest that changes in share prices around non-financial disclosures are influenced by specialist assurance providers. This shows that industry specialisation for non-financial information does not matter to the investors in the absence of the risk of litigation. This means, for assurance of service organisations, which is not mandatory but may be subject to a litigation risk, specialist assurance providers can impact on investors' and other stakeholders' perceptions of the credibility of disclosed information.~~

The following section introduces related assurance standards used for assurance engagements for service organisations.

2.3 Assurance for service organisations: Assurance standard ISAE 3402 and SSEA 16

There are two dominant assurance standards from professional accounting bodies that are largely used for assurance engagements for service organisations. These are International Standard on Assurance Engagements 3402 (ISAE 3402), Assurance Reports on Controls at a Service Organization (IAASB, 2010), and Statement on Standards for Attestation Engagements No. 16 (SSAE 16), Reporting on Controls at a Service Organization (AICPA, 2016). ISAE 3402 is developed by the International Auditing and Assurance Standards Board (IAASB) of the International Federation of Accountants (IFAC), and SSAE 16[1] is developed by the American Institute of Certified Public Accountants (AICPA).

These two standards are assertion-based standards, meaning that they require the management of the service organisations (i.e. the audited organisations) to provide a written assertion regarding relevant controls and procedures. The main difference between ISAE 3402 and SSAE 16 is that they are used by companies in different regions. ISAE 3402 has become the preferred standards for non-US companies, while SSAE 16 has been widely used by firms in the US. However, it is said that the development of SSAE 16 has been adjusted based on the requirements in ISAE 3402; therefore, there is little difference between the two assurance standards (Chuprunov, 2013).

[1] The AICPA first launched SSAE 16 to replace Statement on Auditing Standards No. 70 (SAS 70).

ISAE 3402 is arguably the most used subject-specific international standard for assurance reporting for investment managers and for internal controls over financial reporting (Assure UK, 2017). In the UK, ISAE 3402 is largely used together with the guidance produced by the Audit and Assurance Faculty (AAF) of the Institute of Chartered Accountants in England and Wales (ICAEW), AAF 01/06, to give assurance over financial controls of third-party pension administrators. Whilst the assurance framework is subject to much debate, many of these reports are currently produced in accordance with the explicit guidance, AAF 01/06. They are commonly referred to as 'Assurance Report on Internal Controls (AAF 01/06)'.

ISAE 3402 identifies five primary responsibilities of service organisations. These include: 1) preparing and presenting a complete and accurate description of their internal control frameworks; 2) specify the control objectives; 3) identifying the risks relating to the control objectives; 4) designing, implementing and maintaining controls; 5) providing a written assertion to accompany the description as to the completeness and accuracy of the information provided and stating the criteria used as a basis for making the assertion (IAASB, 2010).

For ISAE 3402, the focus is mainly on the services that affect internal controls relating to financial reporting. There is a distinction between two types of ISAE 3420 assurance reports.

> Type 1 – provides a report on the description and design of controls in a service organisation;
>
> Type 2 – provides a report on the description, design and operating effectiveness of controls in a service organisation.

This means the auditor issuing Type 1 report aims to express their opinion on whether the controls are fairly presented and designed to achieve specific goals at *a specific point in time*. For Type 2 report, the auditor needs to express their opinion on the same issues stated for the Type 1 report, and the operating effectiveness of the tested controls *during a specific period*. The auditor, hence, need to provide the results of the tests. Thus, the type of this assurance report may depend on the need of the audited organisations, and their agreement with the service auditors. However, Type 2 reports are more prevalent as it involves more extensive testing by service auditors.

ISAE 3402 reports were mainly used in the asset management and pension administration industry until 2008. Since then, the demand for ISAE 3402 has expanded to the financial market with financial institutions like real estate management, hosting providers, and credit management institutions demanding ISAE 3402 assurance engagements (ISAE 3402.co.uk, 2014).

The guidance for SSAE 16 has two major elements, which are the SSAE 16 standard itself and the related guide, titled "Service Organizations – Applying SSAE No. 16, Reporting on Controls at a Service Organization". Also the trust service principles (TSP) are used as criteria for evaluation. The criteria included in the TSP are security, availability, processing integrity, confidentiality, and privacy.

For SSAE 16, there are three distinct types of service organisation control report (or assurance for service organisations):

1. SOC 1 Report – provides information to management of service organisations, user organisations, user auditors, and related regulators on the internal controls that affect user organisations' financial statements. The distribution of the report is restricted. ISAE 3402 is an international equivalent to SOC 1. The SOC 1 assessment was actually developed from this standard, but differs from it slightly.
2. SOC 2 Report – provides information to management of service organisations, user organisations, user auditors, and related regulators on non-financial controls that affect data security, privacy, availability, confidentiality and processing integrity (collectively called trust service criteria). The report verifies the application and implementation of controls.
3. SOC 3 Report – provides information to the public on non-financial controls and verifies whether the controls that are applied and implemented are effective in achieving their selected objectives. This report only contains management's assertion that they have met the requirements of the chosen criteria and the auditor's opinion on this assertion.

Hence, ISAE 3402 reports (both Type 1 and Type 2) can be matched with SOC 1 report as they focus "on the controls at a service organization that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting" (IAASB, 2010, pp.323).

As depicted in Figure 1 in Section 2.1 that ~~T~~the commissioners of this kind of assurance engagement are generally service organisations. However, it may be the case that a user entity commissions an auditor to conduct this kind of assurance on the service organisation, if they have specific requirements (ISAE 3402.co.uk, 2014). The former case happens when service organisations want to demonstrate their internal control efficiency and to assure potential clients about the security of their systems. Also, they might commission the assurance to respond to a specific request from the related user entity or the user entity's auditor as illustrated in the process 5.1 and 5.2 in Figure 1. The latter case happens when a user organisation has specific requirements and wants to make sure that the service organisations they are using, or will be using, have appropriate controls over their internal systems in place. It is worth noting ~~that~~ all these differences (e.g. assurance standards, types of assurance reports, and commissioners of assurance engagement) so that different purposes and requirement of specific assurance engagement can be highlighted. ~~two kinds of assurance engagement for service organisations are different because the commissioners, report users, and related stakeholders may be different, hence highlighting different purposes of this kind of assurance engagement.~~

3. Research framework

This paper adopts the notion of accountability to make sense of organisational relationships in the context of assurance practice for service organisations, as accountability can be a proxy for trust, to assure that one party is accountable for their duty towards another party (Swift, 2001). Swift (2001) highlights two conceptualisations of trust that can be related to two kinds of accountability.

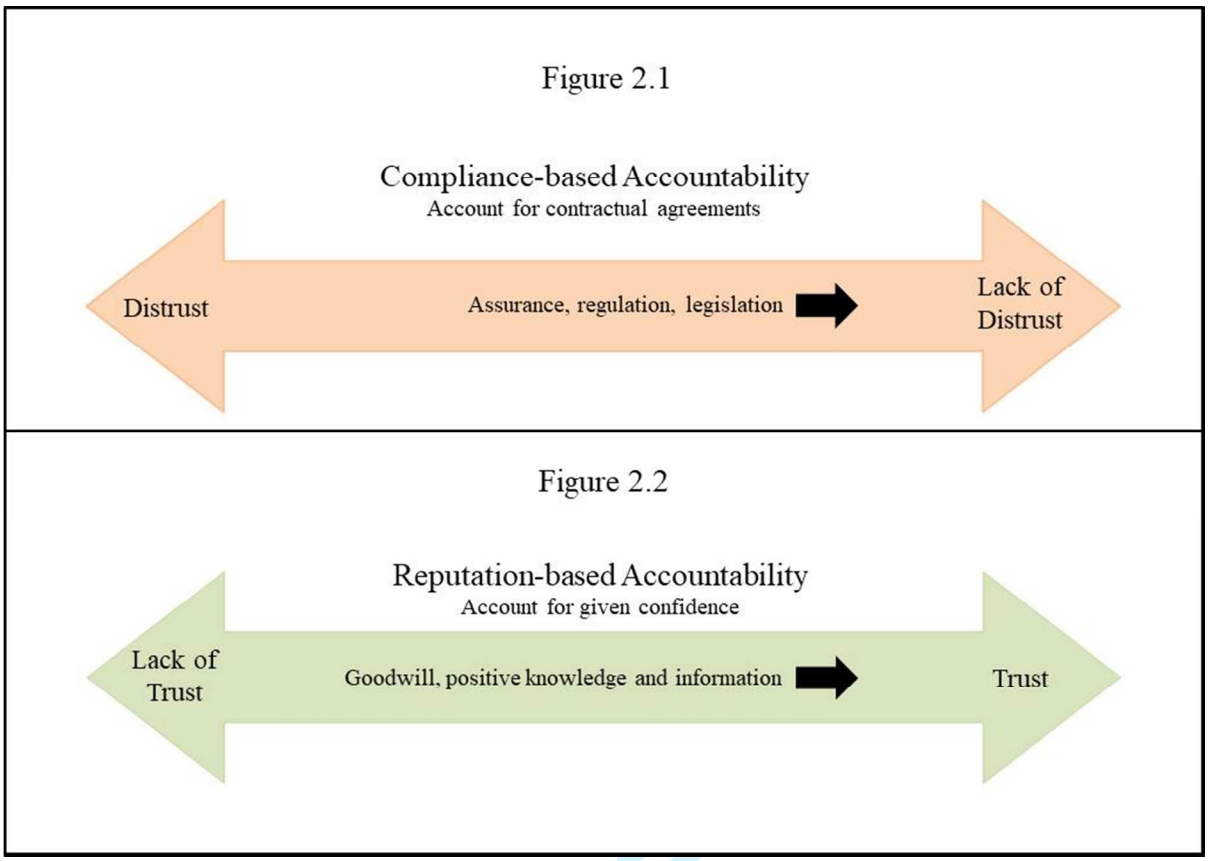
The first conceptualisation is based on the traditional agent-principal view that trust occurs between two parties. The actions of an agent are driven by self-interest and opportunism; therefore, it is difficult or expensive for the principal to verify what the agent is doing, which creates a risk for principals, particularly when there is high information asymmetry in favour of agents and goal conflicts among members (Eisenhardt, 1989). This influences the principal to believe that the agent will pursue self-interest, so the assumption is based on distrust. Trust here refers to "confidence expectation based upon predictability of agent's behaviour" (Zucker, 1986 as cited in Swift, 2001). As distrust is a basis for the call for accountability and is fundamental to the agent-principal assumption, the continuum of trust has distrust on one end, and lack of distrust on the other. Here, trust refers to predictability. This degree of predictability (or trust) can be enhanced by the use of accountability enhancing tools, such as assurance by independent third parties, regulations or related legislation.

This conceptualisation of accountability and trust is normally based on two parties that have a contractual agreement (i.e. agent and principal). Problems between the two parties arise when one party, the principal, delegates work to another party, the agent (Eisenhardt, 1989). The issue of accountability and trust becomes more complicated for new organisational forms, where there might be more than one agent and / or principal, so that the process of holding the agent(s) accountable involves more than one control relationship (Child and Rodrigues, 2003). This includes the operating environment where a service organisation or outsourcing is involved, because responsibilities are (directly or indirectly) delegated to parties other than the agent.

Thus, the second conceptualisation of trust is useful for understanding this complex relationship. Trust here can also refer to "confident expectation based upon agent's goodwill" (Ring and Van de Ven 1992 as cited in Swift, 2001). Trust, therefore, can also represent reliance or confidence. With this definition of trust, two parties are considered interdependent. This richer concept of trust takes into account mutual risks for all involved parties. The continuum of trust in this conceptualisation has trust on one end, and lack of trust on the other.

Figure 2 shows the two ways to conceptualise trust as discussed above. Figure 2.1 illustrates 'compliance-based accountability' as a proxy for the distrust and lack of distrust continuum, while Figure 2.2 illustrates 'reputation-based accountability' as a proxy for the lack of trust and trust continuum.

Figure 2: Accountability as a proxy for trust.



These split continua of trust portray two kinds of accountability, one based on predictability of agents' actions and the other based on a relationship of interdependency among the involved parties, are useful as lenses to understand the purpose of assurance practice as an accountability mechanism.

The analysis and discussion is based on the characteristics of assurance reports (or SOC reports), online news and articles. From this evidence, the accountability of user organisations and service organisations, and trust among related stakeholders, can then be inferred.

The discussion which follows in the next section represents a contextualisation of the aforementioned textual sources using the framework of accountability discussed previously in section 2, in order to examine the purpose of assurance engagements for service organisations. The analysis draws on the work of Swift (2001) to discuss the use of assurance reports as accountability and trust making mechanisms, in particular in the context of entities using service organisations.

4. Example cases: assurance statements for service organisations

Unlike other assurance statements included in annual reports or other forms of corporate report (e.g. assurance for sustainability reports), this kind of assurance report needs to be specifically

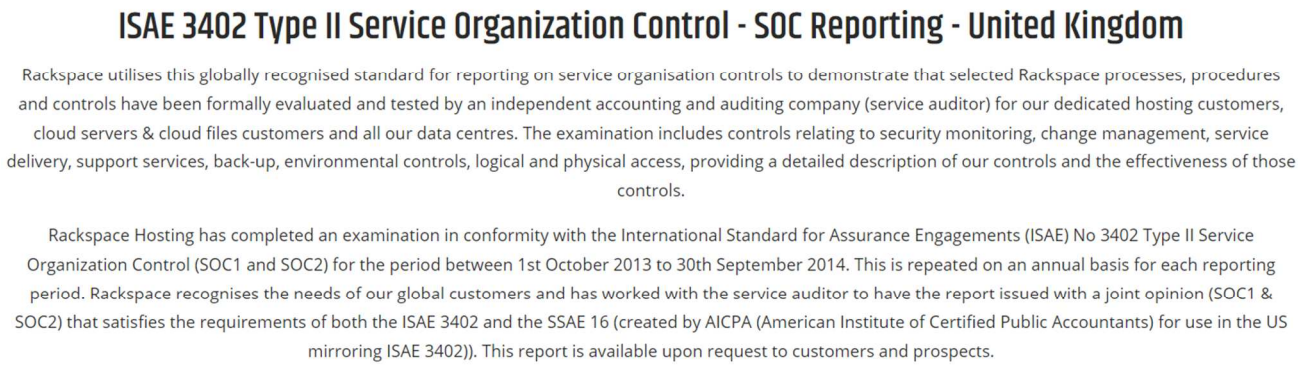
searched for, and there is no database that collectively stores these assurance statements. Also, some types of assurance reports, as mentioned in Section 2.3, are not publicly available. Drawing on the analysis of a large group of reports is difficult due to this lack of access.

Thus, about 20 assurance reports relating to assurance for service organisations are examined. These are supported by additional information from news reports, professional service providers' websites, blogs, and other related online sources. In this paper, although assurance standards are used as a way to categorise assurance reports, the distinction between reports based on ISAE 3402 and SSAE 16 has not been made explicitly and extensively in the empirical cases because the focus is generally on the purpose of the assurance report (or SOC report). The analysis includes publicly available reports / assurance statements based on both ISAE 3402 and SSAE 16.

4.1 ISAE 3402 Assurance Report

The full assurance reports for the assurance engagements for service organisations based on ISAE 3402 are not normally disclosed to the public. However, service organisations publicise the fact that they have commissioned independent assurance providers to examine and assess their control systems. Full assurance reports can also be requested by current or prospective clients.

Figure 3: Excerpt from Rackspace's website.



(Source: https://www.rackspace.com/en-gb/certifications/isae-3402-type-ii-service-organization-control-soc2-reporting-uk (Rackspace, 2017))

From the statement included on the website of Rackspace, a cloud computing service provider (see Figure 3), it can be seen that this service organisation promotes the fact that they have had an independent third party evaluate their internal controls to ensure their effectiveness. They have also included the assurance standards used in the statement, and brief details about the assured areas of their services. However, they did not mention the name of their service auditor in the statement.

A similar scenario is seen with Clearstream Banking Luxembourg, a securities services provider. The assurance report is available to only 'premium users'. However, the service organisation has

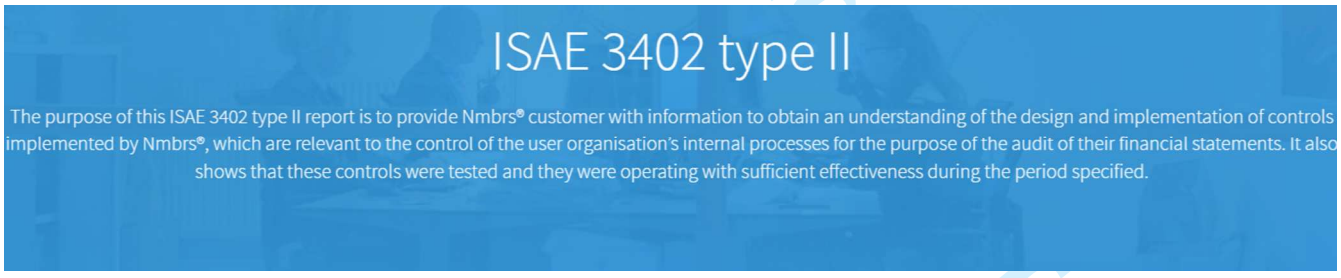
also added a description of the assurance standard used for the assurance engagement (see Figure 4).

Figure 4: Excerpt from Clearstream Banking Luxembourg's website.

(Source: http://www.clearstream.com/clearstream-en/about-clearstream/regulation--1-/isae-report (Clearstream Banking Luxembourg, 2017))

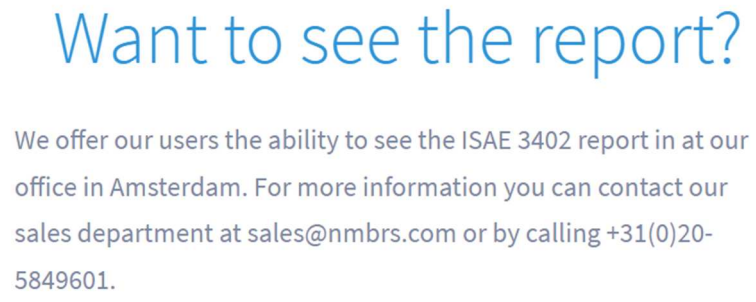
Another company, Nmbrs, which provides cloud HR and payroll software, also publicises the commissionin of a service auditor to conduct an assurance engagement based on ISAE 3402, and states the purpose of the ISAE 3402 report. Still, the report is only available for the users of their services upon request, or at their Amsterdam office.

Figure 5: Excerpt from Nmbrs' website I.



(Source: http:// https://www.nmbrs.com/nl/isae-3402 (Nmbrs, 2017))

Figure 6: Excerpt from Nmbrs' website II.



(Source: http:// https://www.nmbrs.com/nl/isae-3402 (Nmbrs, 2017))

Limitations in access to assurance reports might be a way to limit reputation-based accountability because the name of service auditor is not exposed to the public, but only to limited groups of report users. Similarly, service organisations can limit their accountability to users of their services (i.e. user organisations). However, their actions or internal control mismanagement can also indirectly affect the shareholders and / or stakeholders of user organisations.

One of the reasons that service organisations do not disclose assurance reports may be that they need consent from the service auditor to share these reports with other parties. The following section illustrates the kind of reports that are available via the internet.

4.2 Publicly available ISAE 3402 reports with AFF 01/06

There are some assurance reports for service organisations that are publicly disclosed. However, these reports are usually based on ISAE 3420 and on ICAEW Technical Release, AAF 01/06 Assurance Reports on Internal Controls of Service Organizations Made Available to Third Parties.

Figure 7: Excerpt from KPMG's assurance report in Barnett Waddingham LLP's Assurance Report on Internal Controls 2013/2014.

Dear Sirs

AAF01/06 and ISAE 3402 Type II Reporting Accountants' Assurance Report

Use of report

This report is made solely for the use of the members, as a body, of Barnett Waddingham LLP ("Barnett Waddingham"), and solely for the purpose of reporting on the internal controls of Barnett Waddingham, in accordance with the terms of our engagement letter dated 24 March 2014 and attached as appendix B (together with Additional Terms of Business appended thereon).

Our work has been undertaken so that we might report to the members those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, by the members at their discretion to customers of Barnett Waddingham using Barnett Waddingham's administration activities ('customers'), and to the auditors of such customers, to enable customers and their auditors to verify that a report by reporting accountants has been commissioned by the members of Barnett Waddingham and issued in connection with the internal controls of Barnett Waddingham, and without assuming or accepting any responsibility or liability to customers or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the members as a body and Barnett Waddingham for our work, for this report or for the conclusions we have formed.

(Source: Barnett Waddingham LLP's Assurance Report on Internal Controls 2013/2014 (Barnett Waddingham, 2014))

In the assurance statements by independent assurance providers for this kind of assurance practice, a 'Use of Report' section is usually included. Referring to Figure 7, an assurance report by KPMG for Barnett Waddingham LLP, a provider of actuarial, administration and consultancy services, KPMG allows the user organisation (i.e. Barnett Waddingham LLP) to share the report with other parties. However, there is a caveat limiting their responsibility to the management or members of reporting organisations. The sharing of this report with the public is only to inform the public that the user organisation has commissioned the service auditor to conduct the assurance.

In this case, the users of the report ~~might~~ cannot be clearly or completely specified~~identified~~. The service auditor might, therefore, need to add such a caveat to limit their potential liability from potential unknown stakeholder groups (e.g. different types of customers of Barnett Waddingham LLP). Unlike the case of financial audit practice, in which financial auditors usually address their reports to shareholders of companies, this service ~~user~~ auditor addresses the report to the management of the service~~user~~ organisation to limit their responsibility only to the management of the service organisation. ~~One of the reasons for this might be that they cannot specify certain user groups of the report.~~

Unlike the statements in section 4.1, Figure 7~~X~~ shows that the company discloses the information about who the service auditor is. This means the service auditor might be held accountable for their service by the users of this report. Even though they are not contractually accountable because they have addressed the assurance engagement to the user organisation and because have included a written statement limiting the use of the report and limiting their responsibility, they are still subject to public accountability due to their reputation as a service auditor.

To access this report, potential users do not need to send a request, as is required for the reports in Figures 3 to 6. However, the report needs to be specifically searched for; it is not straightforward to find on the company's website.

There are cases in which service auditors may have some idea of who the users are. Figure 8 shows an assurance report by Assure UK for RPMI Limited, a pension scheme service provider. This report is also based on ISAE 3402 and AAF 01/06; therefore, the report is available for public access. The section, 'Use of Report' is also included and is similar to the report in Figure 7. However, the content about sharing the report is slightly different in that the service organisation has to ask permission from the service auditor to share the report.

Figure 8: Excerpt from Assure UK's assurance report in RPMI Limited's Internal Control Assurance Report 2013/2014.

Reporting accountants' assurance report on internal controls of service organisation to the directors of RPMI Limited

Use of report

This report is made solely for the use of the directors, as a body, of RPMI Limited (RPMI), and solely for the purpose of reporting on the internal controls of RPMI in accordance with the terms of our engagement letter dated 1 July 2014 and found on pages 61-70.

Our work has been undertaken so that we might report to the directors those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, to the Railways Pension Trustee Company Limited (RPTCL) and clients (using RPMI's pensions administration services) (clients), and to the auditors of RPTCL and such clients to enable RPTCL, clients and their auditors to verify that a report by reporting accountants has been commissioned by the directors of RPMI and issued in connection with the internal controls of RPMI and without assuming or accepting any responsibility or liability to clients or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the directors as a body and RPMI for our work, for this report or for the conclusions we have formed.

(Source: RPMI Limited's Internal Control Assurance Report 2013/2014 (RPMI, 2014))

The service auditor permits the sharing of this report to the Railways Pension Trustee Company Limited and the service organization's clients. This shows that the service auditor certainly know about one group of report users. Still, the other groups including potential customers of the service organization can still access the report via the internet.

4.3 Publicly available SSAE16 and SOC 3 reports

As mentioned in section 2.3, assurance engagements for service organisations in the US are usually based on SSAE 16 and are in the format of a service organisation control (SOC) report. The criteria for assurance assessment are based on the TSP. As mentioned before, a SOC 3 report is similar to a SOC 2 report; however, service organisations can distribute SOC 3 reports freely. A SOC 3 report only provides information about whether the service organisation has met the TSP criteria or not. The report is less detailed than SOC 1 and SCO 2 reports. Figures 9 to 11 illustrate excerpts from SOC 3 reports for Amazon Web Service Inc, Google Inc, and Dropbox Inc.

Figure 9: Excerpt from EY's assurance report for Amazon Web Services Inc's Service Organisation Control (SOC) 3 Report 2016/2017.

Report of Independent Accountants

To the Board of Directors of Amazon Web Services, Inc.

We have examined management's assertion that Amazon Web Services, Inc. (AWS), during the period October 1, 2016 through March 31, 2017, maintained effective controls to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS' commitments and system requirements,
- the Amazon Web Services System was available for operation and use to meet AWS' commitments and system requirements, and
- information within the Amazon Web Services System designated as confidential was protected to meet AWS' commitments and system requirements

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of AWS' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Amazon Web Services' relevant security, availability, and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

(Source: Amazon Web Services Inc's Service Organization Control (SOC) 3 Report 2016/2017 (Amazon Web Services, 2017))

Figure 10: Excerpt from EY's assurance report for Google Inc's Service Organisation Control (SOC) 3 Report 2015/2016.

Report of Independent Accountants

To the Management of Google Inc.:

We have examined management's assertion that Google Inc. (referred to hereafter as "Google") during the period 1 May 2015 through 30 April 2016, maintained effective controls to provide reasonable assurance that:

- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements
- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System was available for operation and use to meet the entity's commitments and system requirements
- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements
- information within the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System designated as confidential was protected to meet the entity's commitments and system requirements

based on the criteria for security, availability, processing integrity and confidentiality in the American Institute of Certified Public Accountants' (AICPA) TSP Section 100, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Google Inc.'s management. Our responsibility is to express an opinion based on our examination.

(Source: Google Inc's Service Organization Control (SOC) 3 Report 2015/2016 (Google, 2016))

Figure 11: Excerpt from EY's assurance report for Dropbox Inc's Service Organisation Control (SOC) 3 Report 2015/2016.

Report of Independent Accountants

Management of Dropbox, Inc.

We have examined management's assertion that Dropbox, during the period October 1, 2015 through September 30, 2016 maintained effective controls to provide reasonable assurance that:

- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system was protected against unauthorized access, use, or modification
- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system was available for operation and use as committed or agreed
- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system processing was complete, valid, accurate, timely, and authorized
- Information within the Dropbox Business, Dropbox Enterprise, and Dropbox Education system designated as confidential was protected as committed or agreed
- Personal information within the Dropbox Business, Dropbox Enterprise, and Dropbox Education system was collected, used, disclosed, and retained as committed or agreed

based on the criteria for security, availability, processing integrity, confidentiality, and privacy in the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Dropbox's management. Our responsibility is to express an opinion based on our examination.

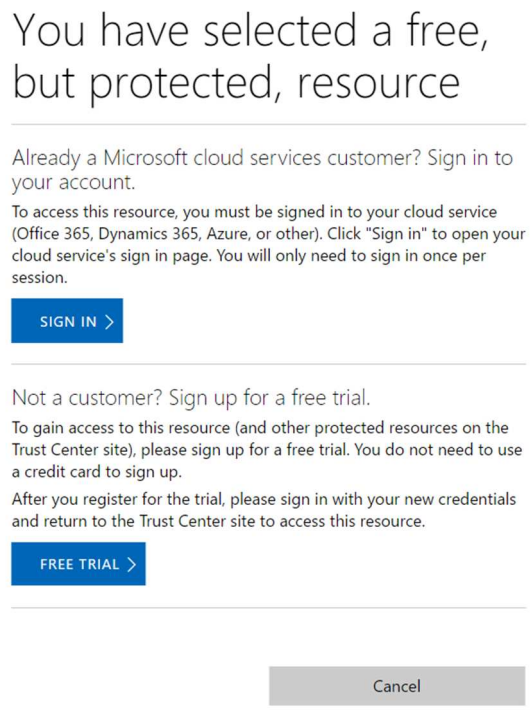
(Source: Dropbox Inc's Service Organization Control (SOC) 3 Report 2015/2016 (Dropbox, 2016))

It can be seen from these excerpts that the addressees of the assurance reports are still the management of the service organisations, unlike with financial audit reports. These reports begin with statements saying that the service auditors have examined assertions by the management of the service organisations to form their assurance opinions.

These assurance engagements are assertion-based. Thus, users of assurance reports need to be aware of and to understand management assertions, as these assurance reports need to be used together with the assertions. However, assertion-based assurance engagements seem to provide better governance of controls as the management of service organisations possess primary responsibility over internal controls and criteria rather than assigning this responsibility to the service auditors (Jones and Iwasaki, 2011).

Although Figures 9 to 11 show SOC 3 reports that are publicly available, there are other service organisations that may not allow direct access to assurance reports. For example, the SOC 3 of Microsoft was also available; however, access to the report can be gained only via a registered account. As the author has an individual user account with Microsoft, the SOC 3 report could be accessed. Figure 12 shows the pop-up message displayed when the author attempted to download the SOC 3 report. This shows that Microsoft's SOC 3 report is only available to Microsoft customers.

Figure 12: Screenshot from Microsoft Inc's website.



(Source: https://www.microsoft.com/en-us/trustcenter/compliance/soc?downloadDocument=nli&documentId=f804ea5a-8846-486c-9d9f-d72020a4e2d6 (Microsoft, 2017))

Unlike the cases of Google Inc and Dropbox Inc, Microsoft asks users who want access to the SOC 3 report to sign a non-disclosure agreement. Thus, an excerpt of the report is not included in this paper. The content of Microsoft's SOC 3 report is similar to that of the Google Inc and Dropbox Inc reports. Although the service auditor is a different firm, it is one of the Big 4 firms.

Being a registered customer of Microsoft, the author also tried to download the SOC 2 report. The download was successful; however, access to the file was denied because the type of license held by the author, that of an individual customer, does not match the license requirements to view the file.

Besides the commissioning of assurance engagements by service organisations, as illustrated above, there may be cases of user organisations themselves, if they have specific assurance requirements, commissioning assurance providers as the service auditors. However, the evidence for this is not clear because such reports cannot be found publicly. This is inferred from the description of the ISAE 3420 assurance standard on the website "ISAE 3402.co.uk" (ISAE 3402.co.uk, 2014), which states that "[w]ithout a Service Auditor's Report, the user organization would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures".

From the examples of assurance statements, access to this kind of assurance report is ubiquitously not straight forward for all stakeholders. Thus, questions about the purpose of assurance, and the accountability of different parties can be raised. Also, caveats regarding inherent limitations on the subject matters of assurance engagements (i.e. internal controls) may introduce questions and doubts about the value and relevance of the information in assurance reports (see Figure 13 as an example of such a statement).

Figure 13: Excerpt II from EY's assurance report for
Amazon Web Services Inc's Service Organisation Control (SOC) 3 Report 2016/2017.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

(Source: Amazon Web Services Inc's Service Organization Control (SOC) 3 Report 2016/2017 (Amazon Web Services, 2017))

This issue is also linked to questions about the frequency of assurance and sufficiency of the efforts of user organisations and service auditors to improve their ability to detect and resist cyber-attacks that may be caused by the vulnerability of internal controls in these service organisations. This also applies to the possibility and means of advancing assurance practice and service organisations' efforts to prevent, resist and respond to real-time cyber security threats.

5. Public disclosure of the assurance and stakeholders' trust

The cases introduced show current assurance practice for service organisations. The main aim of assurance practice is to create trust in itself and trust in related parties (Power, 2003). Trust in service organisations is important for user organisations, while trust in user organisations is important for stakeholders. In the context of information systems and data security, it is therefore important that service organisations and user organisations communicate the effectiveness of their internal controls to assure stakeholders about their plans for preventing and reacting to cyber security threats. Assurance reports on the effectiveness of service organisations' internal controls are one of the communication tools for assuring stakeholders about this. However, the accessibility of such assurance reports is not straightforward. Access is usually limited to particular groups of users. This therefore raises questions about stakeholder communication and about the accountability of service organisations and their auditors to related stakeholders.

As evidenced by assurance statements, service organisations have contract-based accountability to user organisations because user organisations are their direct commissioners. Also, service auditors have contract-based accountability to service organisations for the same reason. However, accountability beyond contractual agreement also needs to be considered in this case because stakeholders of user organisations at the same time can be stakeholders of service organisations.

The empirical cases highlight~~s~~ the fact that assurance statements for service organisations mainly provide reputation-based, not contract-based, accountability between service auditors and user organisations; and between service organisations and user organisations' stakeholders (who can also be service organisations' stakeholders). Limited access to the assurance reports and limited responsibility of service auditors potentially decrease the degree of this reputation-based accountability. The findings reveal a potential accountability paradox regarding the role of assurance practice, as to whether it serves as a managerial tool to build trust or as an accountability mechanism for stakeholders. Current assurance practice seems to be failing to enhance this reputation-based accountability. In some cases, stakeholders do not even know the identities of related service organisations and related service auditors because of the lack of public disclosure.

However, for some cases, reputation-based accountability is enhanced by the use of this assurance for service organisations. With acknowledgement that service organisations have their internal controls assured by independent third parties, stakeholders might have more trust in their systems, even though they do not have contractual-binding agreements with them. Also, the goodwill of service auditors, especially of the Big 4 firms, can enhance such trust because of their credibility and expertise as assurance providers (Hodge et al., 2009).

Another concern relates to stakeholders who are not internet users, as these kinds of assurance reports are mainly available online. However, there are also stakeholder groups not using the internet that might potentially be affected by data security breaches due to the mismanagement of service organisations' internal controls. An example of this is when a person makes a paper-

based registration for a service, and the data is stored in a cloud system. How would service organisations and user organisations communicate this to these groups of stakeholders?

According to the split continua of trust by Swift (2001) discussed in Section 3, the function of this assurance practice for service organisations can be divided into two broad aspects. On one hand, it can be treated as assurance mechanism that helps eliminate distrust between contractual parties. Thus, this kind of relationship forms a compliance-based accountability. On the other hand, the assurance practice seems to be merely additional disclosure of corporate information informing stakeholders that the organisation has this assurance in place. This information, about having the assurance but not publicly providing full details, can potentially create more trust without explicit contractual binding; therefore, the assurance in this case can represent reputation-based accountability.

Limited accessibility of assurance reports and limited responsibility of service auditors bring into question the purpose of assurance practice as an accountability enhancement mechanism, especially for reputation-based accountability. Seeing the reports, knowing who the service auditors are, and reading the content of the reports provide more information to stakeholders and leads them to put their trust in auditors' reputations. In order to create trust for both related organisation and the assurance practice, there is a need to develop better mechanisms to enhance stakeholder dialogue (Swift, 2001).

With this, the purpose of assurance practice and assurance statements can be questioned as to whether they are accountability enhancement tools or serve other purposes. Are they purely a risk management tool for service organisations and / or another kind of consulting service provided by service auditors? Or are they purely marketing tools for service organisations? This is illustrated by a statement in the AICPA's flyer that "[SOC 3] can be used in a service organization's marketing efforts" (AICPA, 2014). In this case, the purpose of the assurance is focused on being a managerial tool to enhance stakeholders' trust without any relation to their accountability.

6. Conclusion

The purpose of this paper has been to provide an overview of assurance practice for service organisations as this assurance practice is important in the digital era, in which data security breaches and outsourcing activities are prevalent. The paper highlights issues relating to the accountability of this contemporary form of organisational relationship that may involve more than one party to be held accountable (e.g. user organisation, service organisation, and auditor). The accountability framework articulated by Swift (2001) provides a useful lens through which to conceptualise accountability in such an environment, which is based on contractual agreement and the goodwill of service organisations, user organisations and their auditors.

The examples of assurance reports demonstrate limited access to such reports, limited contractual accountability to stakeholders of service auditors (which is common in ~~non-financial~~voluntary assurance cases), and limited reputational accountability due to limited

disclosure of information. Also, assurance reports are addressed to service organisations instead of to the wider users of the reports. This means service auditors are contractually responsible for the service organisation only. Does this mean their role is to serve as business advisors or as guardians of public accountability (Humphrey and Moizer, 1990)?

Generally, the benefit of assurance by an independent third party is primarily to enhance confidence in information for the benefit of users of this information or, as is the case in this paper, to provide confidence in specific internal controls of service organisations. Thus, assurance can serve as accountability tools to ensure the audited parties are accountable for their actions that can affect related stakeholders. This kind of assurance practice particularly benefits organisations operating in industries in which there has been increasing scrutiny by different stakeholder groups (Jones and Iwasaki, 2011).

This highlights the nature of this kind of assurance in that it is more or less one-way accountability and communication that provides "rituals of verification" (Power, 1997) instead of fostering trust and accountability through genuine stakeholder dialogue. Assurance reports for service organisations can serve as a reputation-based trust mechanism helping clients or user organisations to choose their service providers. However, the current practice seems insufficient for other important purposes relating to accountability.

The examples and analysis in this paper provide a brief overview of one of the assurance practices that is relevant to modern businesses which are prone to data security threats. Future research in this area is needed in order to understand the usefulness, trust, and accountability relating to these assurance practices. Research work engaging with report users, both individual and institutional, is necessary to understand the usefulness of, and the demand for, the assurance, as well as the trust in specific service organisations and assurance providers. This kind of research can inform the real purpose of assurance reports. Also, it is important for researchers to engage with service organisations to explore requests for these assurance reports from different stakeholders. This again can provide useful information about the purpose of and demand for the practice, whether it provides real value to stakeholders or is just another "ritual of verification" (Power, 1997).

References

AICPA (2014), "*Service Organisation Control Reports - Flyer*" [Online]: AICPA. available at: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/SOC_Reports_Flyer_FINAL.pdf.

AICPA (2016), "Reporting on Controls at a Service Organization", *AT Section 801 Reporting on Controls at a Service Organization*, AICPA.

Amazon Web Services (2017), "Service Organization Controls 3 (SOC 3) Report".

Assure UK (2017), "*ISAE 3000 & 3402*" [Online]. available at: https://www.assureuk.co.uk/what-we-offer/assurance-reporting/isae-3000/ (Accessed 2 June 2017).

Barnett Waddingham (2014), "Assurance Report on Internal Controls (AAF 01/06 and ISAE3402)".

Barrett, M. and Gendron, Y. (2006), "WebTrust and the "commercialistic auditor": The unrealized vision of developing auditor trustworthiness in cyberspace", *Accounting, Auditing & Accountability Journal,* Vol. 19 No. 5, pp. 631-662.

Bierce, W. B. and Kenerson, M. L. (2010), "*Belt and Suspenders, and From SOX to SOC's: Changes in Service Audit Standards on the Service Organization's Risk Management, Security and Process Controls*" [Online]. available at: http://www.outsourcing-law.com/tag/aicpa/ (Accessed 26 July 2017).

Child, J. and Rodrigues, S. B. (2003), "Corporate Governance and New Organizational Forms: Issues of Double and Multiple Agency", *Journal of Management and Governance,* Vol. 7 No. 4, pp. 337-360.

Chuprunov, M. (2013), "IT General Controls in SAP ERP", *Auditing and GRC Automation in SAP*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 131-163.

Clearstream Banking Luxembourg (2017), "*Clearstream Banking Luxembourg ISAE 3402 Report*" [Online]. available at: http://www.clearstream.com/clearstream-en/about-clearstream/regulation--1-/isae-report (Accessed 5 June 2017).

Dropbox (2016), "Service Organization Controls 3 (SOC 3) Report".

Eisenhardt, K. M. (1989), "Agency Theory: An Assessment and Review", *The Academy of Management Review,* Vol. 14 No. 1, pp. 57-74.

Elliott, R. (1977), "Assurance Service Opportunities: Implications for Academia", *American Accounting Association: Accounting Horizons,* Vol. 11 No. 4, pp. 61-74.

Gendron, Y. and Barrett, M. (2004), "Professionalization in Action: Accountants' Attempt at Building a Network of Support for the WebTrust Seal of Assurance*", *Contemporary Accounting Research,* Vol. 21 No. 3, pp. 563-602.

Gonzalez, R., Gasco, J. and Llopis, J. (2010), "Information systems outsourcing reasons and risks: a new assessment", *Industrial Management & Data Systems,* Vol. 110 No. 2, pp. 284-303.

Google (2016), "Service Organization Controls 3 (SOC 3) Report".

Gray, R., Owen, D. and Maunders, K. (1988), "Corporate Social Reporting: Emerging Trends in Accountability and the Social Contract", *Accounting, Auditing & Accountability Journal,* Vol. 1 No. 1, pp. 6-20.

Hodge, K., Subramaniam, N. and Stewart, J. (2009), "Assurance of Sustainability Reports: Impact on Report Users' Confidence and Perceptions of Information Credibility", *Australian Accounting Review,* Vol. 19 No. 3, pp. 178-194.

Humphrey, C. and Moizer, P. (1990), "From techniques to ideologies: An alternative perspective on the audit function", *Critical Perspectives on Accounting,* Vol. 1 No. 3, pp. 217-238.

IAASB (2010), "International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Oganization", IFAC.

ISAE 3402.co.uk (2014), "*What is ISAE 3402?: ISAE 3402 and Outsourcing*" [Online]. available at: http://isae3402.co.uk/what-is-isae3402 (Accessed 2 June 2017).

Jones, M. and Iwasaki, J. (2011), "Governance benefits of new assurance reports", *International Journal of Disclosure and Governance,* Vol. 8 No. 1, pp. 4-15.

Knolmayer, G. F. and Asprion, P. (2011), "Assuring Compliance in IT Subcontracting and Cloud Computing", in Kotlarsky, J., Willcocks, L. P. and Oshri, I. (Eds.) *New Studies in Global IT and Business Service Outsourcing: 5th Global Scourcing Workshop 2011, Courchevel, France, March 14-17, 2011, Revised Selected Papers*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 21-45.

Microsoft (2017), "*Microsoft Trust Center: SOC 1, 2, and 3 Reports*" [Online]. available at: https://www.microsoft.com/en-us/trustcenter/compliance/soc?downloadDocument=nli&documentId=f804ea5a-8846-486c-9d9f-d72020a4e2d6 (Accessed 7 June 2017).

Nmbrs (2017), "*ISAE 3402 Type II*" [Online]. available at: https://www.nmbrs.com/nl/isae-3402 (Accessed 5 June 2017).

Panth, D., Mehta, D. and Shelgaonkar, R. (2014), "A survey on security mechanisms of leading cloud service providers", *International Journal of Computer Applications,* Vol. 98 No. 1.

Power, D. and Terziovski, M. (2007), "Quality audit roles and skills: Perceptions of non-financial auditors and their clients", *Journal of Operations Management,* Vol. 25 No. 1, pp. 126-147.

Power, M. (1996), "Making things auditable", *Accounting, Organizations and Society,* Vol. 21 No. 2–3, pp. 289-315.

Power, M. (1997), "Expertise and the construction of relevance: Accountants and environmental audit", *Accounting, Organizations and Society,* Vol. 22 No. 2, pp. 123-146.

Power, M. K. (2003), "Auditing and the production of legitimacy", *Accounting, Organizations and Society,* Vol. 28 No. 4, pp. 379-394.

Rackspace (2017), "*ISAE 3402 Type II Service Organization Control - SOC Reporting - United Kingdom*" [Online]. available at: https://www.rackspace.com/en-gb/certifications/isae-3402-type-ii-service-organization-control-soc2-reporting-uk (Accessed 5 June 2017).

Roberts, J. and Scapens, R. (1985), "Accounting systems and systems of accountability — understanding accounting practices in their organisational contexts", *Accounting, Organizations and Society,* Vol. 10 No. 4, pp. 443-456.

RPMI (2014), "Assurance Report on Internal Controls (AAF 01/06 and ISAE3402)".

Swift, T. (2001), "Trust, reputation and corporate accountability to stakeholders", *Business Ethics: A European Review,* Vol. 10 No. 1, pp. 16-26.

Assurance for Service Organizations: Contextualizing Accountability and Trust

Edits are in the paper – Edited as marked by the reviewer's editorial changes

Comments from the email/note:

Needs a bit more connection in the text to issues of cyber assurance. For instance, assurance of software and hardware that will be used. This may be a bit more critical than just non-financial information assurance.

I tried to make more connection to the cybersecurity issues and expand the limited/captured term of "non-financial reporting". The paper mainly highlights the practice of assurance for service organisation in relation to the business environment where cyber security is prevalent. Thus, it is one form of preventive/assurance mechanism that relate to cyber security and (cyber) trust. I have added some text to address this comment, but I am not sure I fully address this point and improve the paper sufficiently in the direction that you want. Please kindly let me know what you think.

Major Questions (from the attached review document):

1) So the Type 1 and 2 reports do not deal with non-financial controls that SOC 2 reports do. Type 2 reports seem to subsume Type 1 reports. Most organizations would seem to need Type 2 reports??? Correct?

See the additional text in Section 2.3. You are right the Type 2 subsume Type 1 report. The choice of specific types of report depends on the need to organisations, and maybe recommendation and their discussion with the auditor. However, Type 2 reports are more prevalent as it provides more extensive testing by the service auditor.

For ISAE 3402, Type 1 report includes auditor's opinion a specific point in time on description and design of controls; while Type 2 report includes the issue in Type 1, please the test on operating effectiveness of controls over a specific period.

ISAE 3402 (Type 1 and 2) cane be more closely matched with SOC 1 as they are dealing with the controls relevant to financial reporting; while SOC 2 engagement is based on the security, availability, processing integrity, confidentiality or privacy. These principles extend the concerns beyond financial reporting to include non-financial related controls.

2) In regard to Ferguson and Pundrich could cybersecurity risk be related to litigation? Especially with the concern for data protection?

No, they did not refer directly to cyber security and data protection. But it refers specifically to geological assurance experts to make the inference about the non-financial assurance and expertise of the auditor. They found that in the areas where litigation risks are absence, the expertise does not really play a big part.

I have excluded the paper, rewritten the paragraph to be more related to the cyber security issues.

3) Could the discussion of section 2.3 be related to figure 1?

Please see additional text in the paper.

4) Though certain reports are not required to be disclosed and there is no contractual relationship – can't service organizations disclose the information? If it is a public organization I can get their reports. For instance, I can get the GRI report.

They (Public organisations) may have this kind of reports (e.g. ISAE 3402, SOC2), but there is not regulation enforcing them to disclose it. For the cases that I mentioned, companies limit the access to the assurance reports. One of the reasons might be that those reports might contain detailed information so they think limited access is better than open access because they can track to whom the information get exposed to. The genuine reasons for this might need to gain from interviews with them or their auditors to get more precise insights. That is why SOC 3 is specifically designed assurance report for public use, as it contains less detailed information than SOC 2 does.

For GRI: I would say this is slightly different from GRI report in the way that GRI is voluntary 'reporting' framework, not assurance standards. A company can do GRI reporting with or without assurance engagement. Generally, when they have assurance report accompanying their GRI reports, they usually disclose the assurance opinion/report/statement. I was told by the sustainability/GRI report auditors from one of the Big4 firm here that sometimes companies chose not to disclose the assurance statements. One of the reasons might be that they get unfavorable/qualified opinion. As there is no regulation to provide such an assurance with the report; they chose not to disclose but explain that they are improving the process and skip the assurance this year.

5) Are there penalties for disclosure of these reports to others?

To my knowledge, there are no such penalties. See the answer for the previous question regarding why companies might not want to disclose the full report (but just disclose only the fact that they have commissioned the assurance engagement). Also, from the auditors' point of view, they might want to limit the exposure of the report as well so that they can avoid the public assuming their responsibility (albeit they have put caveat in their report), and better manage the expectation gap.

Assurance for Service Organisations: Contextualising Accountability and Trust

Submission for Managerial Accounting Journal

Special issue: Cybersecurity Risks, Controls and Assurance

Figure 1. Relationships between service organisations and other entities.

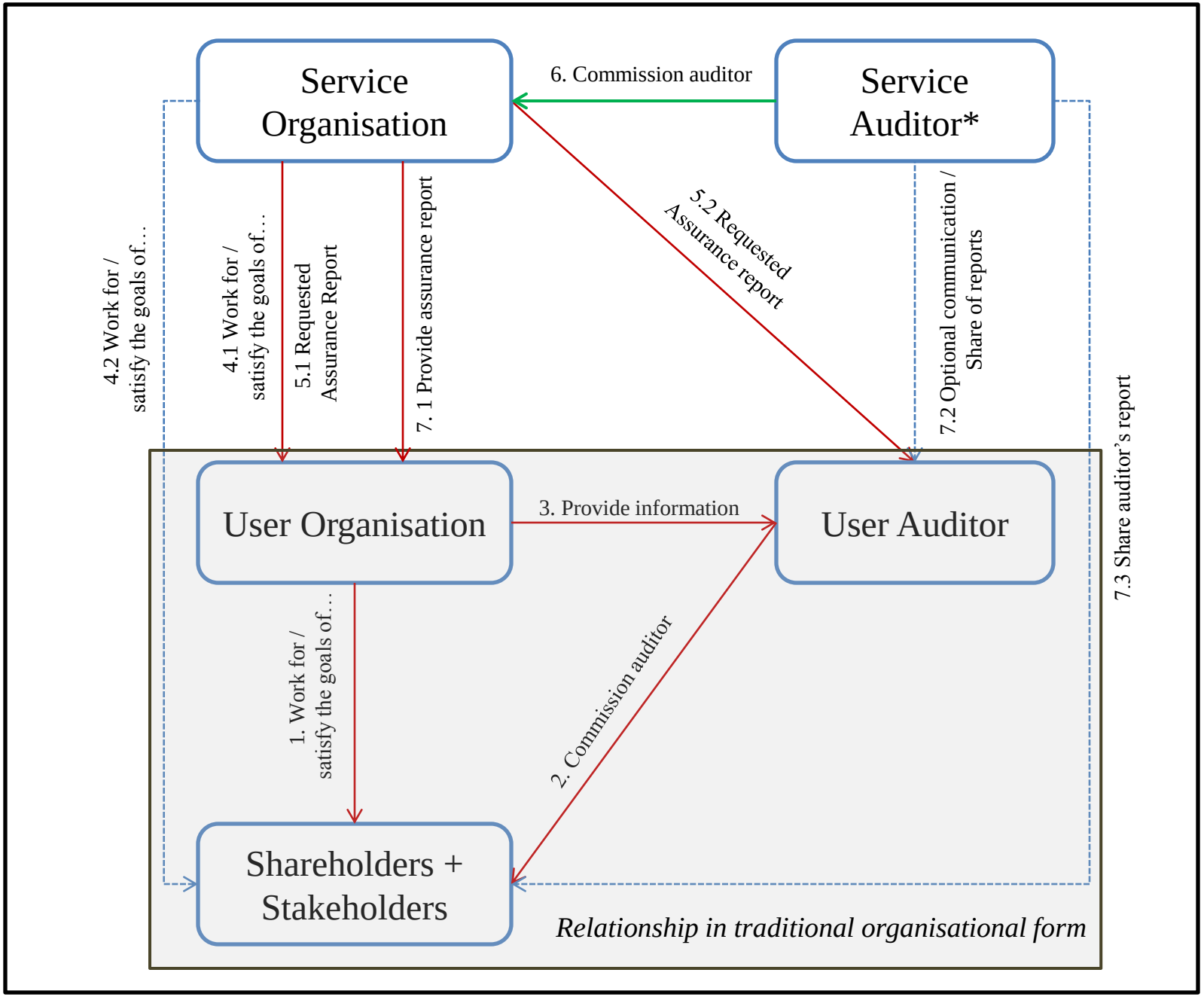


Figure 2: Accountability as a proxy for trust.

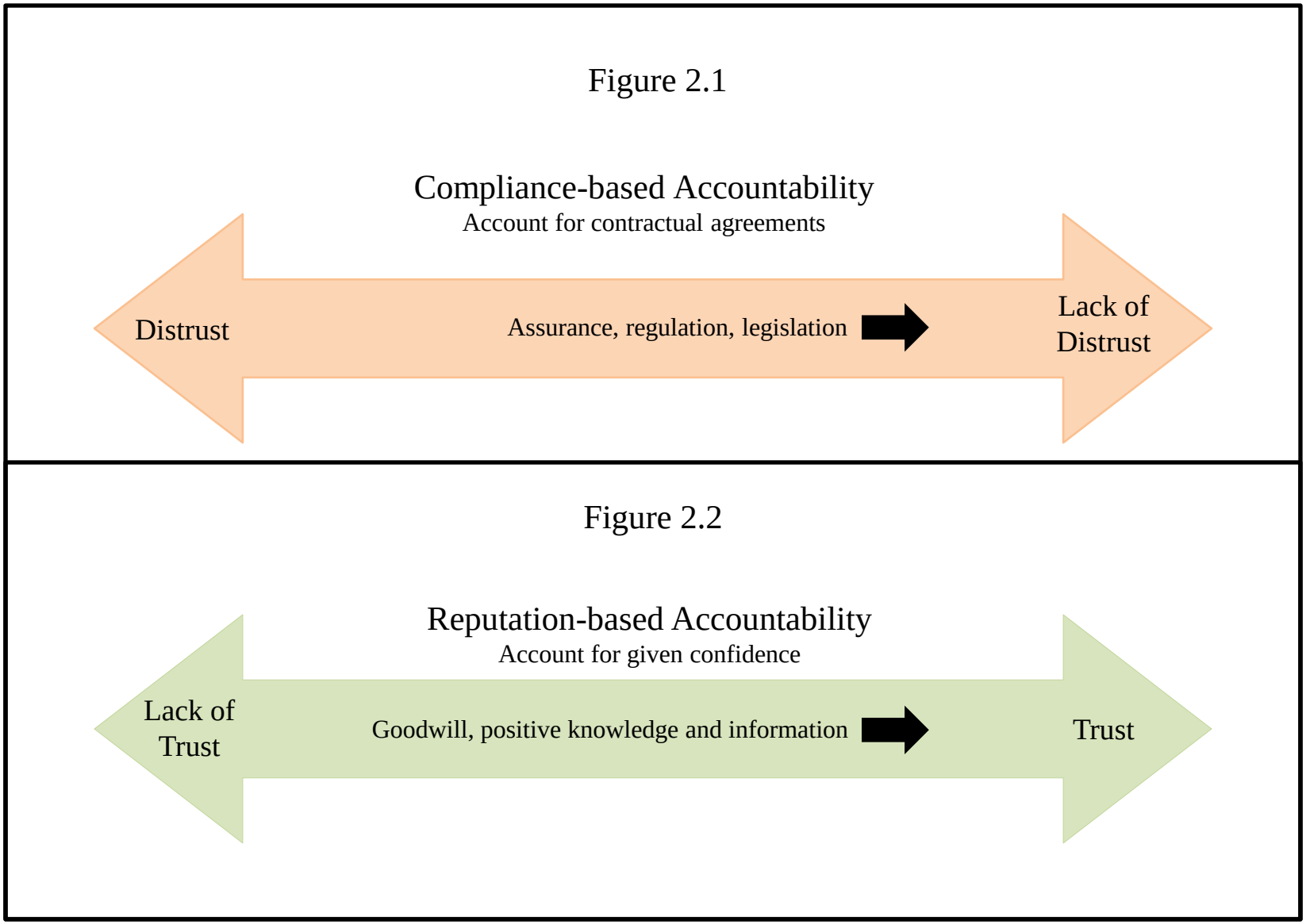
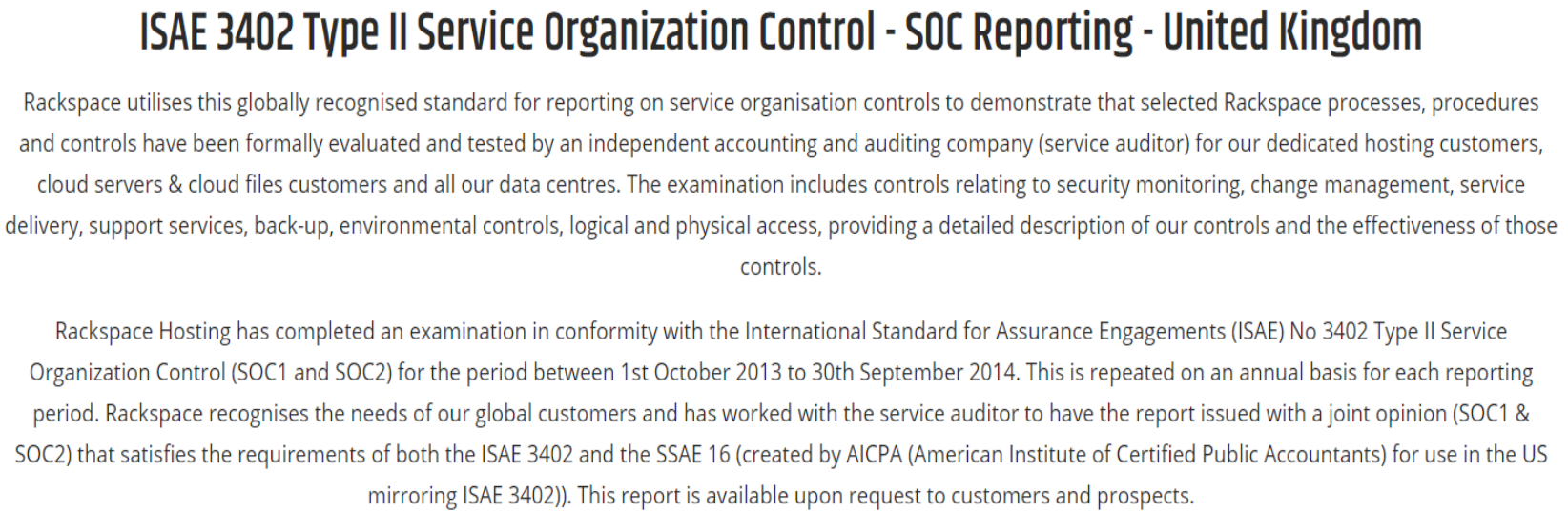


Figure 3: Excerpt from Rackspace's website.



ISAE 3402 Type II Service Organization Control - SOC Reporting - United Kingdom

Rackspace utilises this globally recognised standard for reporting on service organisation controls to demonstrate that selected Rackspace processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing company (service auditor) for our dedicated hosting customers, cloud servers & cloud files customers and all our data centres. The examination includes controls relating to security monitoring, change management, service delivery, support services, back-up, environmental controls, logical and physical access, providing a detailed description of our controls and the effectiveness of those controls.

Rackspace Hosting has completed an examination in conformity with the International Standard for Assurance Engagements (ISAE) No 3402 Type II Service Organization Control (SOC1 and SOC2) for the period between 1st October 2013 to 30th September 2014. This is repeated on an annual basis for each reporting period. Rackspace recognises the needs of our global customers and has worked with the service auditor to have the report issued with a joint opinion (SOC1 & SOC2) that satisfies the requirements of both the ISAE 3402 and the SSAE 16 (created by AICPA (American Institute of Certified Public Accountants) for use in the US mirroring ISAE 3402)). This report is available upon request to customers and prospects.

Figure 4: Excerpt from Clearstream Banking Luxembourg's website.

Clearstream Banking Luxembourg ISAE 3402 Report

27.04.2017

The attached document **will only be visible in the Attachments section below if logged in as a Premium User** and contains the following information:

The International Standard on Assurance Engagements (ISAE) No. 3402, is an assurance report on the description of controls, their design and operating effectiveness.

This report is intended for customers who have used Clearstream's system, and their auditors. It provides them with valuable information regarding Clearstream's controls and the effectiveness of those controls, through a detailed description and an independent assessment of whether the controls placed in operation, were suitably designed, and operated effectively.

Figure 5: Excerpt from Nmbrs' website I.

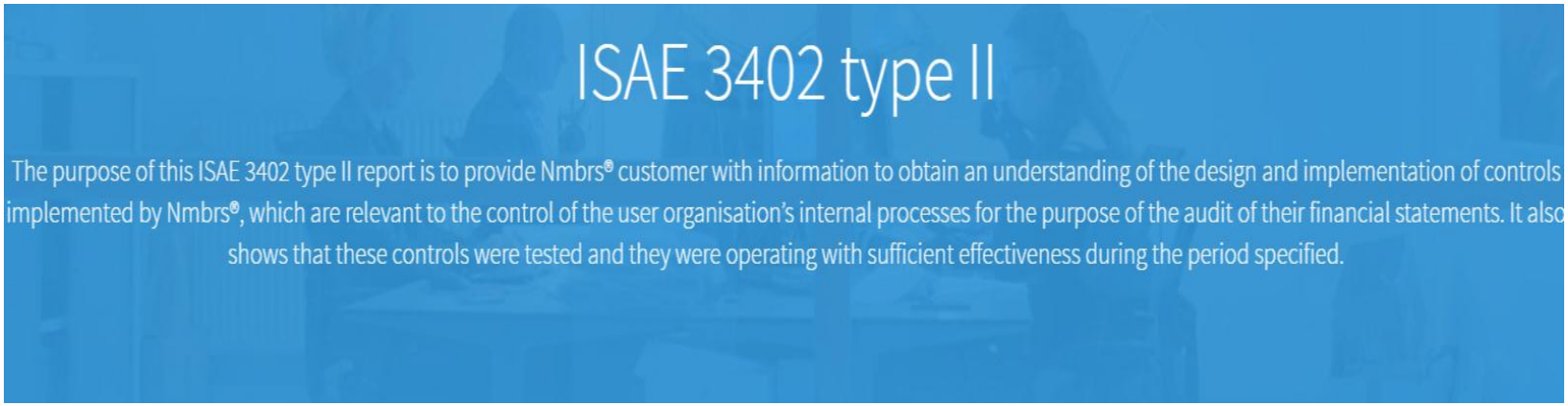


Figure 6: Excerpt from Nmbrs' website II.

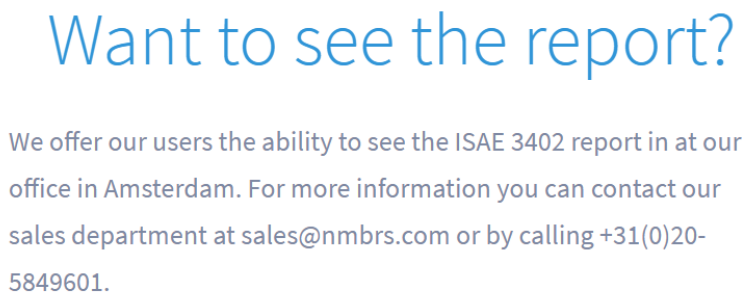


Figure 7: Excerpt from KPMG's assurance report in Barnett Waddingham LLP's Assurance Report on Internal Controls 2013/2014.

Dear Sirs

AAF01/06 and ISAE 3402 Type II Reporting Accountants' Assurance Report

Use of report

This report is made solely for the use of the members, as a body, of Barnett Waddingham LLP ("Barnett Waddingham"), and solely for the purpose of reporting on the internal controls of Barnett Waddingham, in accordance with the terms of our engagement letter dated 24 March 2014 and attached as appendix B (together with Additional Terms of Business appended thereon).

Our work has been undertaken so that we might report to the members those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, by the members at their discretion to customers of Barnett Waddingham using Barnett Waddingham's administration activities ('customers'), and to the auditors of such customers, to enable customers and their auditors to verify that a report by reporting accountants has been commissioned by the members of Barnett Waddingham and issued in connection with the internal controls of Barnett Waddingham, and without assuming or accepting any responsibility or liability to customers or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the members as a body and Barnett Waddingham for our work, for this report or for the conclusions we have formed.

Figure 8: Excerpt from Assure UK's assurance report in RPMI Limited's Internal Control Assurance Report 2013/2014.

Reporting accountants' assurance report on internal controls of service organisation to the directors of RPMI Limited

Use of report

This report is made solely for the use of the directors, as a body, of RPMI Limited (RPMI), and solely for the purpose of reporting on the internal controls of RPMI in accordance with the terms of our engagement letter dated 1 July 2014 and found on pages 61-70.

Our work has been undertaken so that we might report to the directors those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, to the Railways Pension Trustee Company Limited (RPTCL) and clients (using RPMI's pensions administration services) (clients), and to the auditors of RPTCL and such clients to enable RPTCL, clients and their auditors to verify that a report by reporting accountants has been commissioned by the directors of RPMI and issued in connection with the internal controls of RPMI and without assuming or accepting any responsibility or liability to clients or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the directors as a body and RPMI for our work, for this report or for the conclusions we have formed.

Figure 9: Excerpt from EY's assurance report for Amazon Web Services Inc's Service Organisation Control (SOC) 3 Report 2016/2017.

Report of Independent Accountants

To the Board of Directors of Amazon Web Services, Inc.

We have examined management's assertion that Amazon Web Services, Inc. (AWS), during the period October 1, 2016 through March 31, 2017, maintained effective controls to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS' commitments and system requirements,
- the Amazon Web Services System was available for operation and use to meet AWS' commitments and system requirements, and
- information within the Amazon Web Services System designated as confidential was protected to meet AWS' commitments and system requirements

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of AWS' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Amazon Web Services' relevant security, availability, and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Figure 10: Excerpt from EY's assurance report for Google Inc's Service Organisation Control (SOC) 3 Report 2015/2016.

Report of Independent Accountants

To the Management of Google Inc.:

We have examined management's assertion that Google Inc. (referred to hereafter as "Google") during the period 1 May 2015 through 30 April 2016, maintained effective controls to provide reasonable assurance that:

- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements
- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System was available for operation and use to meet the entity's commitments and system requirements
- the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements
- information within the Google Apps for Work, Google Drive for Work, Google Apps for Education, Google Cloud Platform, and Other Google Services System designated as confidential was protected to meet the entity's commitments and system requirements

based on the criteria for security, availability, processing integrity and confidentiality in the American Institute of Certified Public Accountants' (AICPA) TSP Section 100, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Google Inc.'s management. Our responsibility is to express an opinion based on our examination.

Figure 11: Excerpt from EY's assurance report for Dropbox Inc's Service Organisation Control (SOC) 3 Report 2015/2016.

Report of Independent Accountants

Management of Dropbox, Inc.

We have examined management's assertion that Dropbox, during the period October 1, 2015 through September 30, 2016 maintained effective controls to provide reasonable assurance that:

- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system was protected against unauthorized access, use, or modification
- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system was available for operation and use as committed or agreed
- The Dropbox Business, Dropbox Enterprise, and Dropbox Education system processing was complete, valid, accurate, timely, and authorized
- Information within the Dropbox Business, Dropbox Enterprise, and Dropbox Education system designated as confidential was protected as committed or agreed
- Personal information within the Dropbox Business, Dropbox Enterprise, and Dropbox Education system was collected, used, disclosed, and retained as committed or agreed

based on the criteria for security, availability, processing integrity, confidentiality, and privacy in the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Dropbox's management. Our responsibility is to express an opinion based on our examination.

Figure 12: Screenshot from Microsoft Inc's website.

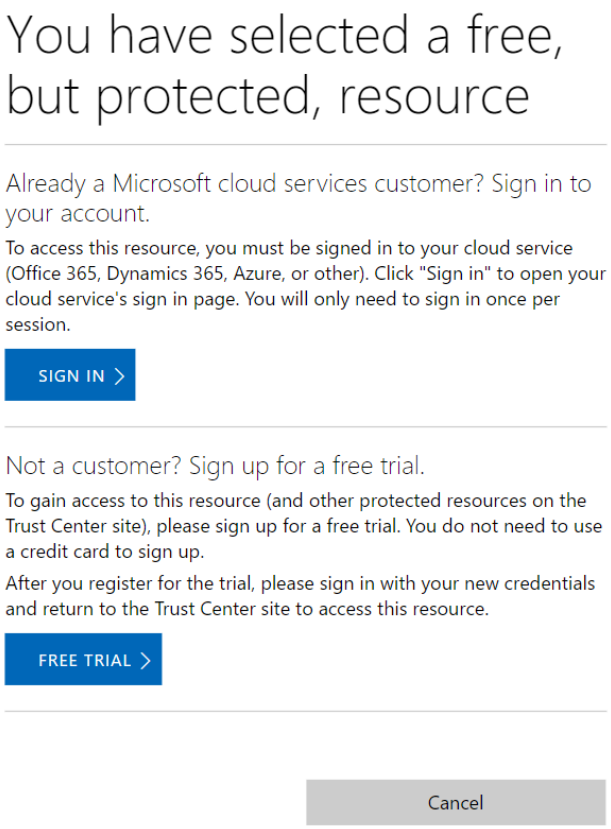


Figure 13: Excerpt II from EY's assurance report for Amazon Web Services Inc's Service Organisation Control (SOC) 3 Report 2016/2017.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.